Lawrence Livermore National Laboratory
Computer Security Organization

Go Ahead, Visit Those Websites, You Can't Get Hurt, Can You?

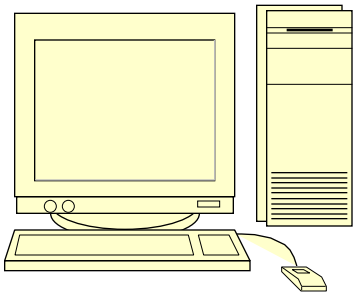
- ***Brief overview of WWW technology***
- ***Recent News***
- ***Web Browsing Guidelines***

James Rothfuss
rothfuss1@llnl.gov
October, 1997

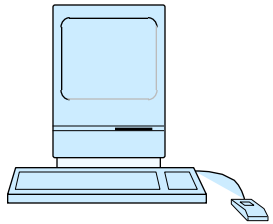
Lawrence Livermore National Laboratory
Computer Security Organization

Webserver <-> Browser

Webserver



Browser



(Netscape Navigator

MS Internet Explorer)

HTML

- Static information, one way
- Forms may request information

CGI

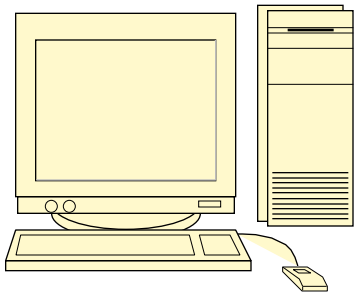
- Dynamic on server side
- Can request information from browser
- No browser resource access
  (unless you explicitly allow file uploads)

Helpers and Plug-ins

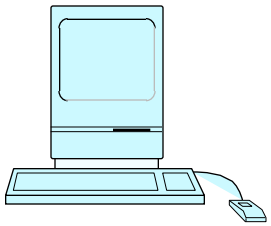
- Static data is downloaded
- The data is run on an EXISTING application.
- Local resource can be accessed

Webserver <-> Browser

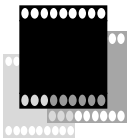
Webserver

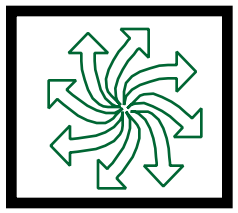


Browser



data & code

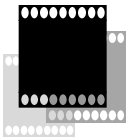


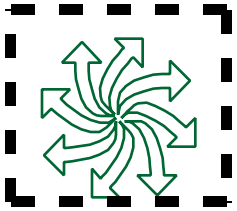


Java, Javascript

- Executable code and data is downloaded.
- Dynamic on browser side
- Can send information either way
- Browser resource access? Depends on browser

data & code





ActiveX

- Dynamic on browser side
- Can send information either way
- Browser resource access? Depends on browser

ActiveX is not a programming language.
It is a set of active client side capabilities.

ActiveX Controls Microsoft describes these as "interactive objects." Takes the place of the old OLE controls. They can be written in almost any popular language.

Documents Desktop documents such as Excel or Word files. ActiveX allows them to be downloaded and viewed through the Web browser.

Java Accepts and runs Java applets.

JScript Microsoft's rendition of JavaScript (The same... but a little different).

VBScript The Visual Basic language embedded directly into HTML documents.

Security

HTML

- Static downloads.
  No real security concerns.

CGI

- Cannot access client side files without permission.

Helpers and Plug-ins

- Full access to local client system.
- Since you download and install them, they are assumed to be trustworthy

Security

continued

Java/Javascript:

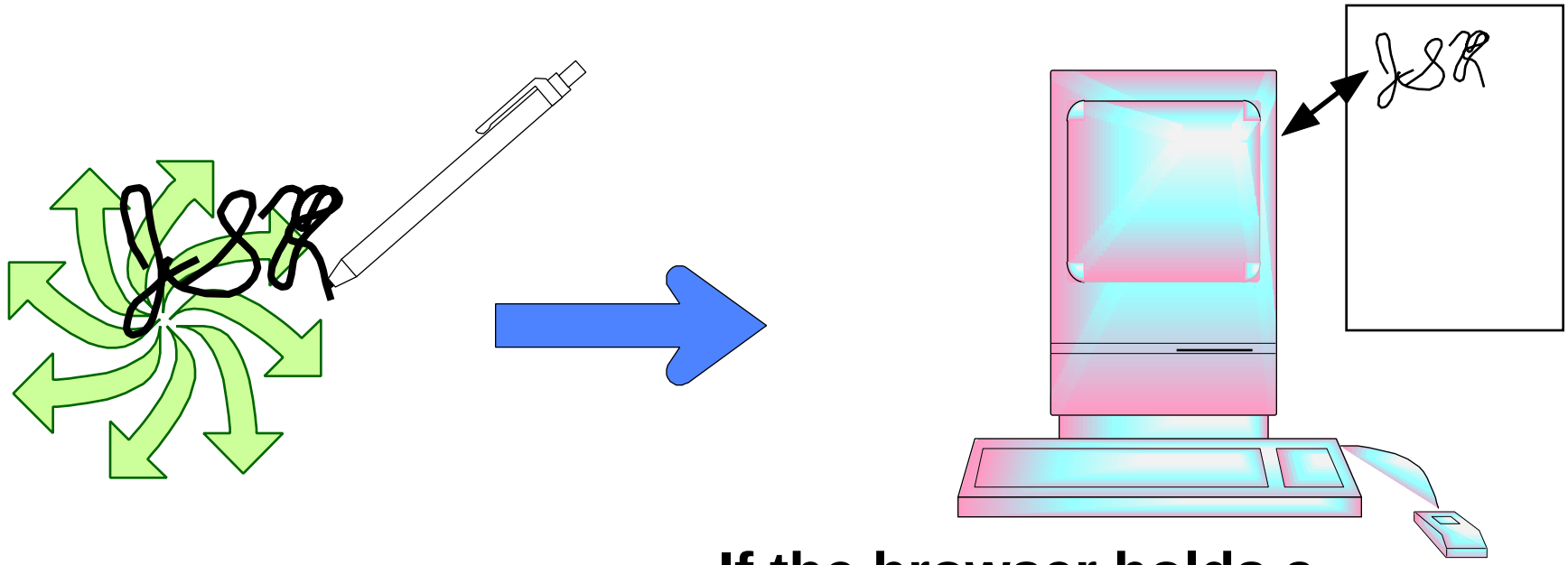
- Netscape Navigator 3.0 - NO READ/WRITE ACCESS on local disk
- Internet Explorer 3.0 - CONFIGURABLE on browser

- Netscape Communicator - The Sandbox gets bigger. Restricted Read/Write

ActiveX (other than Java):

- on Internet Explorer 3.0 - Relies on digital signatures CONFIGURABLE on browser (High, Low, NONE)

Digital Signature



The object (Java, ActiveX) is signed by a registered signature

If the browser holds a matching signature the object will run

NOTE: The signature check can be turned off

Netscape News:

- **Netscape claims they will eventually incorporate some ActiveX functionality.**
- **Netscape will incorporate digital signatures**
- **Netscape will make read/write access optional**

News items

Bugs Found In Java

JavaScript Gives More Than Expected

http://www.osf.org/~loverso/javascript/

Chaos Computer Club has fun with ActiveX

http://www.news.com/News/Item/0,4,7761,00.html

SexyGirls Run Up Phone Charges

http://www.ftc.com/opa/9702/audiotex.htm
http://www.ftc.com/opa/9702/audiotex1.htm
http://www.ftc.com/os/9702/audiotex.htm

more News items

ActiveX Exploder Shuts Down Windows 95

http://www.halcyon.com/mclain/ActiveX

Web Spoofing For Fun

Http://www.cs.princeton.edu/sip/pub/spoofing.html

WindowsNT and 95 Passwords Out

NT - http://www.ntshop.net/security/ie3-4.htm\
BE CAREFUL - THIS SITE STEALS AND POSTS PASSWORDS\
95 - http://www.security.org.il/msnetbreak/

ActiveX Word/Excel Macros Escape Security

http://www.infoworld.com/cgi-bin/displayStory.pl?970324.eiebug.htm

more News items

Internet Explorer Runs Remotely

http://www.cybersnot.com/iebug.html

Internet Explorer Security Disabled

http://www.scv.com.sg/~entea/security/reggap.htm (?)

Firewalls No Help

http://www.alcrypto.co.uk/java
http://www.javaworld.com/javaworld/jw-03-1997/jw-03-securityholes.html

Confidential Information Logged

http://www5.zdnet.com/zdnn/content/inwo/0327/inwo0001.html

ShockWave Delivers a Shock

http://www.webcomics.com/shockwave
http://www.micromedia.com/shockzone/info/security

Attack Speculation

Pumping for Information

"cyber social engineering"

Active, Real-Time Attacks by CGI

Macro Languages Embedded in Helpers and Plug-ins

"mites"
(Shockwave/Lingo)

WWW Conducive to Professional Information Gatherers

You Go to Them

Lawrence Livermore National Laboratory
Computer Security Organization

Web Browsing Guidelines

- **Helper programs and Plug-ins can be Dangerous**
- **Websites Collect Information about YOU**
- **Do Not Let a Website Interrogate You**
- **Java, JavaScript, and ActiveX can be Dangerous**
- **Websites Can Lie**
- **Use Common Sense**
  Stay out of Bad Neighborhoods

Lawrence Livermore National Laboratory
Computer Security Organization